## REMARKS

By this amendment, the claims have generally been amended to remove artifacts of European practice and to be in full compliance with 35 U.S.C. 101.

Amended Independent Claim 14 now recites a method for verifying a signature, or respectively an authentication, utilizing an asymmetric private-key and public-key cryptographic calculation process between a "*prover*" entity and a "*verifier*" entity. The prover entity includes communication means for communicating with said verifier entity, wherein the prover entity performs first cryptographic calculations with said private key to produce a signature calculation, or respectively an authentication value constituting a response value, and the verifier entity, based on said response value, performs second cryptographic calculations with said public key to perform said signature verification, or respectively said authentication, the first and second cryptographic calculations serving to implement the calculation of modulo-n or large-number multiplications, wherein for a cryptographic calculation process using a public key comprising a public exponent e and a public modulo n, and a private key comprising a private exponent, the method further includes calculating at the level of said prover entity at least one prevalidation value and using the communication means of the prover entity for transmitting to the verifier entity, in addition to said signature calculation or response value, at least said one prevalidation value, and utilizing said prevalidation value by the verifier entity to perform at least one modular reduction without any division operation for said modular reduction.

Not only does Ebihara fail to teach or suggest the above combination of featues, but also the prevalidation value as claimed and the calculation at the level of said prover entity at least one prevalidation value. Ebihara discloses that encrypted text CA is forwarded from the transmitting person (A) to the receiving person (B) (See Fig. 2 of Ebihara), however this does not acticipate or render obvious the feature of using the communication means of the prover entity for transmitting to the verifier entity, in addition to said signature calculation or response value, at least said one prevalidation value, and utilizing said prevalidation value by the verifier entity to perform at least one modular reduction without any division operation for said modular reduction as recited in Claim 14.

Moreover, Claim 14 specifically recites that utilizing said prevalidation value by the verifier entity to perform at least one modular reduction is done without any division operation for said modular reduction.

In contradistinction, Ebihara states that Person B receives the encrypted signature text cA (See col. 2, lines 60-65 and Fig. 2 of Ebihara) and then performs operations (See col. 3) without using any additional prevalidation value received from Person A. Since the receiving portion of Ebihara (Person B) necessarily performs division operations, Ebihara suffers from the same drawbacks as discussed in Applicants' specification.

While Menezes, Stinson, Poore and Liskov were cited as supporting references for the various rejections under 35 U.S.C. 103, they at least fail to overcome the deficiencies as noted above.

Claim 14 is thus allowable.

The dependent claims are also allowable for the reasons outlined above and the additional feature(s) recited therein.

With all rejections having been overcome, Applicants respectfully submit the application is in condition for allowance. An early Notice of Allowance is respectfully solicited.

Should the Examiner believe that any further action is necessary to place this application in better form for allowance, the Examiner is invited to contact Applicants' representative at the telephone number listed below.

The Commissioner is hereby authorized to charge to deposit account number 50-1165 (T2146-906752) any fees under 37 CFR § 1.16 and 1.17 that may be required by this paper and to credit any overpayment to that Account. If any extension of time is required in connection with the filing of this paper and has not been separately requested, such extension is hereby requested.

Respectfully submitted,

Date: January 7, 2005

By: ______________________
Edward J. Kondracki
Reg. No. 20,604

Jason H. Vick
Reg. No. 45,285

Miles & Stockbridge, P.C.
1751 Pinnacle Drive
Suite 500
McLean, Virginia 22102-3833
(703) 903-9000